

<b>DEPARTMENT OF DEFENSE</b> <b>CONTRACT SECURITY CLASSIFICATION SPECIFICATION</b> <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				<b>1. CLEARANCE AND SAFEGUARDING</b> a. FACILITY CLEARANCE REQUIRED <div style="text-align: center;">Top Secret</div> b. LEVEL OF SAFEGUARDING REQUIRED <div style="text-align: center;">Secret</div>																																																																																																																																																																									
<b>2. THIS SPECIFICATION IS FOR:</b> <i>(X and complete as applicable)</i>			<b>3. THIS SPECIFICATION IS:</b> <i>(X and complete as applicable)</i>																																																																																																																																																																										
a. PRIME CONTRACT NUMBER		X		a. ORIGINAL <i>(Complete date in all cases)</i>																																																																																																																																																																									
b. SUBCONTRACT NUMBER				DATE (YYYYMMDD) 20040421																																																																																																																																																																									
				b. REVISED <i>(Supersedes all previous specs)</i>																																																																																																																																																																									
				REVISION NO.																																																																																																																																																																									
X c. SOLICITATION OR OTHER NUMBER		DUE DATE (YYYYMMDD)		c. FINAL <i>(Complete Item 5 in all cases)</i>																																																																																																																																																																									
				DATE (YYYYMMDD)																																																																																																																																																																									
<b>4. IS THIS A FOLLOW-ON CONTRACT?</b> <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: Classified material received or generated under _____ <i>(Preceding Contract Number)</i> is transferred to this follow-on contract.																																																																																																																																																																													
<b>5. IS THIS A FINAL DD FORM 254?</b> <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____.																																																																																																																																																																													
<b>6. CONTRACTOR</b> <i>(Include Commercial and Government Entity (CAGE) Code)</i>																																																																																																																																																																													
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>																																																																																																																																																																									
TBD		TBD		TBD																																																																																																																																																																									
<b>7. SUBCONTRACTOR</b>																																																																																																																																																																													
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>																																																																																																																																																																									
N/A		N/A		N/A																																																																																																																																																																									
<b>8. ACTUAL PERFORMANCE</b>																																																																																																																																																																													
a. LOCATION		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>																																																																																																																																																																									
N/A		N/A		N/A																																																																																																																																																																									
<b>9. GENERAL IDENTIFICATION OF THIS PROCUREMENT</b> Consolidated Acquisition of Professional Services (CAPS) Manpower Support																																																																																																																																																																													
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="2"><b>10. CONTRACTOR WILL REQUIRE ACCESS TO:</b></td> <td colspan="2"><b>YES</b></td> <td colspan="2"><b>NO</b></td> <td colspan="2"><b>11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:</b></td> <td colspan="2"><b>YES</b></td> <td colspan="2"><b>NO</b></td> </tr> <tr> <td colspan="2">a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> <td colspan="2">a. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY</td> <td colspan="2"></td> <td colspan="2" style="text-align: center;">X</td> </tr> <tr> <td colspan="2">b. RESTRICTED DATA</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> <td colspan="2">b. RECEIVE CLASSIFIED DOCUMENTS ONLY</td> <td colspan="2"></td> <td colspan="2" style="text-align: center;">X</td> </tr> <tr> <td colspan="2">c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> <td colspan="2">c. RECEIVE AND GENERATE CLASSIFIED MATERIAL</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> </tr> <tr> <td colspan="2">d. FORMERLY RESTRICTED DATA</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> <td colspan="2">d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE</td> <td colspan="2"></td> <td colspan="2" style="text-align: center;">X</td> </tr> <tr> <td colspan="2">e. INTELLIGENCE INFORMATION</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> <td colspan="2">e. PERFORM SERVICES ONLY</td> <td colspan="2"></td> <td colspan="2" style="text-align: center;">X</td> </tr> <tr> <td colspan="2">(1) Sensitive Compartmented Information (SCI)</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> <td colspan="2">f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> </tr> <tr> <td colspan="2">(2) Non-SCI</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> <td colspan="2">g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> </tr> <tr> <td colspan="2">f. SPECIAL ACCESS INFORMATION</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> <td colspan="2">h. REQUIRE A COMSEC ACCOUNT</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> </tr> <tr> <td colspan="2">g. NATO INFORMATION</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> <td colspan="2">i. HAVE TEMPEST REQUIREMENTS</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> </tr> <tr> <td colspan="2">h. FOREIGN GOVERNMENT INFORMATION</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> <td colspan="2">j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> </tr> <tr> <td colspan="2">i. LIMITED DISSEMINATION INFORMATION</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2">k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> </tr> <tr> <td colspan="2">j. FOR OFFICIAL USE ONLY INFORMATION</td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> <td colspan="2">l. OTHER <i>(Specify)</i></td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> </tr> <tr> <td colspan="2">k. OTHER <i>(Specify)</i></td> <td colspan="2" style="text-align: center;">X</td> <td colspan="2"></td> <td colspan="6"> Notification of government security activity is required.  See addendum. </td> </tr> </table>						<b>10. CONTRACTOR WILL REQUIRE ACCESS TO:</b>		<b>YES</b>		<b>NO</b>		<b>11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:</b>		<b>YES</b>		<b>NO</b>		a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		X				a. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY				X		b. RESTRICTED DATA		X				b. RECEIVE CLASSIFIED DOCUMENTS ONLY				X		c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X				c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		X				d. FORMERLY RESTRICTED DATA		X				d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE				X		e. INTELLIGENCE INFORMATION		X				e. PERFORM SERVICES ONLY				X		(1) Sensitive Compartmented Information (SCI)		X				f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X				(2) Non-SCI		X				g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		X				f. SPECIAL ACCESS INFORMATION		X				h. REQUIRE A COMSEC ACCOUNT		X				g. NATO INFORMATION		X				i. HAVE TEMPEST REQUIREMENTS		X				h. FOREIGN GOVERNMENT INFORMATION		X				j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		X				i. LIMITED DISSEMINATION INFORMATION		X		X		k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		X				j. FOR OFFICIAL USE ONLY INFORMATION		X				l. OTHER <i>(Specify)</i>		X				k. OTHER <i>(Specify)</i>		X				Notification of government security activity is required. See addendum.					
<b>10. CONTRACTOR WILL REQUIRE ACCESS TO:</b>		<b>YES</b>		<b>NO</b>		<b>11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:</b>		<b>YES</b>		<b>NO</b>																																																																																																																																																																			
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		X				a. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY				X																																																																																																																																																																			
b. RESTRICTED DATA		X				b. RECEIVE CLASSIFIED DOCUMENTS ONLY				X																																																																																																																																																																			
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X				c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		X																																																																																																																																																																					
d. FORMERLY RESTRICTED DATA		X				d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE				X																																																																																																																																																																			
e. INTELLIGENCE INFORMATION		X				e. PERFORM SERVICES ONLY				X																																																																																																																																																																			
(1) Sensitive Compartmented Information (SCI)		X				f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X																																																																																																																																																																					
(2) Non-SCI		X				g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		X																																																																																																																																																																					
f. SPECIAL ACCESS INFORMATION		X				h. REQUIRE A COMSEC ACCOUNT		X																																																																																																																																																																					
g. NATO INFORMATION		X				i. HAVE TEMPEST REQUIREMENTS		X																																																																																																																																																																					
h. FOREIGN GOVERNMENT INFORMATION		X				j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		X																																																																																																																																																																					
i. LIMITED DISSEMINATION INFORMATION		X		X		k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		X																																																																																																																																																																					
j. FOR OFFICIAL USE ONLY INFORMATION		X				l. OTHER <i>(Specify)</i>		X																																																																																																																																																																					
k. OTHER <i>(Specify)</i>		X				Notification of government security activity is required. See addendum.																																																																																																																																																																							

**12. PUBLIC RELEASE.** Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (Specify)  
ASC/PAX, 1865 4th Street, WPAFB, OH 45433-7129, 937 255-2776 FAX 937 656-4022 <http://ascpa.public.wpafb.af.mil>  
Public release of Sensitive Compartmented Information (SCI) is NOT authorized

No public release of Special Access Required (SAR) or SAR related material is authorized without approval of SAF/AQ through SAF/AQ Security, 2690 Loop Road West, Suite 010, Wright-Patterson AFB OH 45433.  
to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)\* for review.  
\*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

**13. SECURITY GUIDANCE.** The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

The National Industrial Security Program Operating Manual (NISPOM), Jan 95, applies to this request for information.  
a. Ref Blk 10a/11h: COMSEC/Cryptologic Safeguarding requirements apply. See NSA Industrial COMSEC Manual (NSA Manual 90-1), October 2001 for details. For on base performance, COMSEC is incumbent on the government.  
b. Ref Blk 10c: CNWDI Briefing required prior to granting access. See NISPOM Chapter 9 for details.  
c. Ref Blk 10e(1): Contractor requires access to SCI materials; SCI security requirements apply, see SCI addendum for details.  
d. Ref Blk 10e(2): Contractor will require access to intelligence information and must comply with AFI 14-303/AFMC Supplement 1. The Program Manager has determined that disclosure does not create an unfair competitive advantage for the contractor or a conflict of interest with the contractor's obligation to protect the information and will submit the AFMC Form 210 to the ASC SIO (ASC/IN) for approval prior to granting access.  
e. Ref Blk 10f: The NISPOM Supplement (NISPOMSUP), 29 Dec 94, and the DoD overprint to the NISPOMSUP, 1 Apr 04 and applicable Program Security Directives (PSD) and Security Classification Guides (SCG) applies to this contract for Special Access Requirements.  
f. Ref Blk 10g: NATO briefing required prior to granting access: See NISPOM Chapter 10 for details.  
g. Ref Blk 10j: For Official Use Only (FOUO) applies. See addendum.  
h. Ref Blk 10k: Program Protection Plans (PPP) which are applicable will be provided by the Government activity.  
i. Ref Blk 11c: Any classified generated in the performance of this contract shall require the contractor to eith apply derivative classification and markings consistent with the source material. Special considerations apply. See addendum. Performance on base may be "access only" (Block 11a) and the releasing task unit will furnish classification guidance for the service to be performed. All SAR work must be performed in areas approved by SAF/AQ Security.  
j. Ref Blk 11f: Overseas contractor performance will be identified in each task order.  
k. Ref Blk 11i: EMSEC requirements apply. See addendum. For on base performance EMSEC is incumbent on the government.  
l. Ref Blk 11k: DCS address is HQ Defense Courier Service, 830 Chisholm Ave, Ft Meade MD, 20755  
RFI reviewed by Sheryl Baker 88 SFS/SFAS, (937) 255-4729 on 21 Apr 04.  
(See continuation sheet)

**14. ADDITIONAL SECURITY REQUIREMENTS.** Requirements, in addition to ISM requirements, are established for this contract. ☒ Yes ☐ No  
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

a. Ref Blk 10e(1): SCI security requirements may apply in future task orders. Tasking units will provide specific requirements and guidance. See SCI addendum for general guidance.  
b. Ref Blk 10f: Special Access Requirements/Procedures apply. Guidance for gaining access will be provided by the SAF/AQ Security delegated Program Security Officer (PSO) or SAF/AQ Security. (See continuation sheet)

**15. INSPECTIONS.** Elements of this contract are outside the inspection responsibility of the cognizant security office. ☒ Yes ☐ No  
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

a. Ref Blk 10e(1): SCI requirements apply, see SCI addendum (para 13) for details.  
b. Ref Blk 11i: Partial performance will occur at WPAFB, OH. DSS is relieved of all security oversight for performance on the installation. For performance on WPAFB, security oversight will be under the cognizance of 88 SFS/SFAS for non-SAR performance and by SAF/AQ Security for SAR performance.

**16. CERTIFICATION AND SIGNATURE.** Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL  P.S. STRADER	b. TITLE  Contracting Officer	c. TELEPHONE (Include Area Code)  937-656-4433
d. ADDRESS (Include Zip Code) ASC/CXCK 2275 D Street, Bldg 16, Rm 129 Wright-Patterson AFB OH 45433-7233	<b>17. REQUIRED DISTRIBUTION</b> <input checked="" type="checkbox"/> a. CONTRACTOR <input type="checkbox"/> b. SUBCONTRACTOR <input type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR <input type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION <input type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER <input checked="" type="checkbox"/> f. OTHERS AS NECESSARY	
e. SIGNATURE		

**DD Form 254 Continuation Sheet**  
**Request for Information**

Block 13 continued:

- m. Ref Blk 11i: The Notification of Government Security and Visitor Group Security Agreement Clause applies. See Contract Clause in Section I for details.
- n. Functional Area Chief (FAC): Each individual task order will identify the FAC for the tasking unit.
- o. Functional Area Evaluator (FAE): Each individual task order will identify the FAE for the tasking unit.
- p. Ref Blk 17f (Distribution): 88 SFS/SFAS, 1801 Tenth Street, Wright-Patterson AFB OH 45433-7625

Block 14 continued:

- c. Ref Blk 11j: OPSEC requirements may apply in future task orders. Tasking units will provide specific guidance.

**ADDENDUM TO DD FORM 254 (Block 10j)****FOR OFFICIAL USE ONLY (FOUO)***(Reference DoD Regulation 5400.7/Air Force Supplement, 22 July 1999)*

1. **GENERAL:** FOUO is information that has not been given a security classification pursuant to the criteria of an Executive Order, but which may be withheld from the public because disclosure would cause a foreseeable harm to an interest protected by one or more of the Freedom of Information Act (FOIA) exemptions 2 through 9. Additional information on FOUO may be obtained by contacting the User Agency. FOUO is assigned to information at the time it is created in a DoD Agency or derivatively as instructed in a Security Classification Guide.

2. **MARKING:**

a. FOUO information received (released by a DoD component) should contain the following marking, when received: ***THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY DISCLOSURE UNDER FOIA. EXEMPTION(S) \_\_\_\_\_ APPLIES/APPLY.***

b. Mark an unclassified document containing FOUO information "FOR OFFICIAL USE ONLY" at the bottom of each page containing FOUO information and on the bottom of the front page or front cover (if any) and on the back of the last page and on the back cover (if any). Each paragraph containing FOUO information shall be marked as such.

c. Within a classified document, an individual page that contains both FOUO and classified information shall be marked at the top and bottom with the highest security classification of information appearing on the page. Individual paragraphs shall be marked at the appropriate classification level, as well as unclassified or FOUO, as appropriate. An individual page that contains FOUO information but no classified information shall be marked "FOR OFFICIAL USE ONLY" at the top and bottom of the page, as well as each paragraph that contains FOUO information. NOTE: For "production efficiency" the entire document may be marked top and bottom with the highest level of classification contained within it, as long as every paragraph is marked to reflect the specific classification of the information it contains.

d. Mark other records, such as computer print outs, photographs, films, tapes, or slides "FOR OFFICIAL USE ONLY" so that the receiver or viewer knows the record contains FOUO information.

e. Mark each part of a message that contains FOUO information. Unclassified messages containing FOUO information must show the abbreviation "FOUO" before the text begins.

3. **DISSEMINATION:** FOUO may be disseminated between officials of DoD Components, DoD contractors, consultants and grantees to conduct official business for DoD. Recipients shall be made aware of the status of such information and transmission shall be by means that preclude unauthorized public disclosure.

4. **TRANSMISSION:** FOUO information shall be transmitted in a manner that prevents disclosure of the contents. When not commingled with classified information, it may be sent via first-class mail or parcel post. Bulky shipments, i.e. testing materials, that otherwise qualify under postal regulations, may be sent by fourth-class mail. FOUO information may also be sent over facsimile equipment; however, when deciding whether to use this means, balance the sensitivity of the records against the risk of disclosure. Consider the location of sending and receiving machines and ensure authorized personnel are available to receive the FOUO information as soon as it is transmitted. Transmittal documents shall call attention to the presence of FOUO attachments. FOUO information may also be sent via e-mail, if it is sent via a system that will prevent unintentional or unauthorized disclosure.

5. **STORAGE:** To safeguard FOR OFFICIAL USE ONLY records during normal duty hours, place them in an out-of-sight location if your work area is accessible to persons who do not have a valid need for the information. After normal duty hours, store FOUO records to prevent unauthorized access. File them with other unclassified records in unlocked files or desks when normal internal building security is provided. When there is no internal building security, locked buildings or rooms normally provide adequate after-hours protection. If such protection is not considered adequate, FOUO material shall be stored in locked containers such as file cabinets, desks, or bookcases. *Expenditure of funds for security containers or closed areas solely for the protection of FOUO data is prohibited.*

6. **DESTRUCTION:** When no longer needed, FOUO information shall be disposed of by any method that will preclude its disclosure to unauthorized individuals.

**ADDENDUM TO DD FORM 254 (Block 10e(1))**  
**SENSITIVE COMPARTMENTED INFORMATION (SCI) CLAUSES**

1. **Reference Block 14:** AFMAN 14-304; DoD 5105.21-M-1; DCID 6/3, 6/4, 6/8, 6/9, and 1/19; JDCSISSS; and DIAM 50-4 provide the necessary guidance for physical, personnel, industrial, information, and information systems security measures and is part of the Sensitive Compartmented Information (SCI) security specifications for the contract.

2. SCI will not be released to contractor employees without the specific release approval by the originator of the material as outlined in the governing directives and based on prior approval and certification of "need-to-know" by the Contracting Officer's Representative (COR):

TBD under each task order

(Name)	(Office Symbol)	(Phone)
--------	-----------------	---------

3. Names of contractor personnel requiring access to SCI and justification for SCI billets will be submitted for coordination and action to SSO ASC/INS after the contract monitor approval/concurrence. Upon receipt of written approval from the COR, the Contractor Special Security Officer (CSSO) may submit the necessary forms to Defense Security Service (DSS) for a Single Scope Background Investigation (SSBI) for those personnel nominated for SCI access in accordance with the National Industrial Security Program Operating Manual (NISPOM).

4. This contract will require SCI billets in order to fulfill contractual obligations incurred. SCI access is subject to US Government review and approval as outlined in the aforementioned SCI security regulations. Upon completion or cancellation of the contract, the CSSO will debrief all personnel not required for contract closeout and those billets will be disestablished.

5. The CSSO must restrict access to only those individuals who possess the necessary security clearance and who are actually providing services under the contract. Further dissemination to other contractors, sub-contractors, other government agencies, private individuals or organizations is prohibited unless authorized in writing by the releasing agency.

6. SCI materials furnished in support of this contract remains the property of the DoD department or command that released it. Upon completion or cancellation of the contract, all SCI materials furnished will be returned to the direct custody of the originator of the materials.

7. Classified foreign intelligence materials must not be released to foreign nationals or immigrant aliens whether or not they are also consultants, US contractors, or employees of the contractor, regardless of the level of their security clearance, except with advanced written permission from the originator.

8. Inquiries pertaining to classification guidance on SCI will be directed to the COR listed in para 2 above. SCI security management issues shall be directed to SSO ASC/INS, phone (937) 255-3932, DSN prefix 785.

9. An SCI Facility (SCIF) meeting the physical security requirements outlined in DCID 6/9 must be either used for contract work or established and maintained at the contractor location. All SCI used for this contract shall be stored, handled, and maintained in a SCIF, be it the local contractor SCIF or similarly SCI-accredited facilities used by the contractor. Address of SCIF for contract execution: TBD under each task order

10. For contract work within a contractor established SCIF, information systems (computers), electronic connectivity, and similar electronic methods of storing and communicating within and outside the SCIF must be in compliance with DCID 6/3, DIAM 50-4, the JDCSISSS, and any additional instructions issued by DIA/DAC-2A, HQ AFMC/INS, and SSO ASC/INS.

11. The CSSO must maintain accountability for all classified foreign intelligence materials released to their custody.

12. The CSSO must not reproduce classified foreign intelligence without advance approval of the releasing agency. If permission is granted, each copy will be controlled in the same manner as the original. The CSSO must not destroy any classified foreign intelligence without advance approval of the releasing agency.

13. **Reference Block 15:** This contract requires access to SCI. If the contractor has established a SCIF, the Defense Intelligence Agency (DIA) and its designees are responsible for all inspections of the contractor SCIF and SCI security management program for ensuring compliance with all SCI security regulations and policies.

Effective: 12 March 2004

**ADDENDUM TO DD FORM 254 (Blocks 10e(1) and 11c)**  
**SPECIAL CONSIDERATIONS**  
**(AFMAN 33-214V EXTRACT)**

**NOTE:** These considerations are not applicable to performance within a Sensitive Compartmented Information Facility (SCIF). See paragraph 10 of SCI addendum for guidance.

**3.4. Special Items.** People may innocently introduce other radio devices, such as pagers, hand-held portable transceiver radios, cellular telephones, cordless telephones, and cordless microphones into the area processing classified information with disastrous results. Also, alarm systems may use radio transmitters to alert remotely located security or fire-fighting teams.

**3.4.1. Hand-Held Radios.** These countermeasures are required. Hand-held radio transceivers used with intrabase radios and land mobile radios deserve special consideration because of their unique operational applications. A person may carry these devices into an area where classified information is processed. If the person carrying such a device works in the facility, either turn off the device and use the telephone or separate it 2 meters from classified processors: no transmissions are allowed. If the person carrying the device is a short-term visitor, it is not necessary to turn off the radio because the visitor usually moves about in the facility. Infrequent transmissions are allowed, but only for short durations.

**3.4.2. Beepers and Pagers.** These countermeasures are required. Beepers and pagers deserve special consideration because of their unique operational applications. A person may carry these devices into an area where classified information is processed. If the person carrying such a device works in the facility, either turn off the device and use the telephone or keep the device 2 meters from classified processors. If the person carrying the device is a short-term visitor, it is not necessary to turn off the device because the visitor usually moves about in the facility. If the device has a transmit capability, follow the instructions for hand-held radios.

**3.4.3. Alarm Systems.** These countermeasures are required. The mode of operation of alarm systems radio frequency transmitters will determine their treatment. Any such transmitter with a continuous transmit mode or a high duty cycle (transmits most of the time) must meet the same separation requirements as all other fixed transmitters; follow the applicable guidance in paragraph 3.3. If they do not meet these requirements, exclude them from operating in the classified information processing area. Low duty cycle (transmits short bursts infrequently) systems are not considered hazards and require no special treatment.

**3.4.4. Cellular Telephones.** These countermeasures are required. When a cellular telephone is used as an operational necessity separate it 5 meters from RED equipment. When the cellular telephone is a personal asset, its use is prohibited. Disable the unit from receiving calls or separate it 10 meters from RED processors. Cellular telephones are excluded from operating within 10 meters of the classified information processing area when the facility is located outside the United States.

**3.4.5. Cordless Telephones.** These countermeasures are required. When a radio frequency cordless telephone is used as an operational necessity, separate it 5 meters from RED equipment. When the cordless telephone is a personal asset, its use is prohibited. Disable the personal cordless telephone from receiving calls or separate it 10 meters from RED processors. There are no separation requirements for infrared cordless telephones. Cordless telephones are excluded from operating within 10 meters of the classified information processing area when the facility is located outside the United States.

**3.4.6. Cordless Microphones.**

**3.4.6.1. Radio Frequency Cordless Microphones.** These countermeasures are required. When a radio frequency cordless microphone, encrypted or unencrypted, is used for briefing either classified information or unclassified information, separate it 10 meters from RED equipment. Using unencrypted radio frequency cordless microphones for classified briefings is prohibited.

**3.4.6.2. Infrared Cordless Microphones.** These countermeasures are required. Using an infrared cordless microphone for briefing classified information requires blocking the line of sight to a possible place where an adversary could detect the infrared emanations. Do not forget that smooth or shiny surfaces cause infrared signals to be reflected. The best solution is to use a closed room, keeping the doors closed and covering the windows with drapes.

**3.5.7. Cordless Accessories.** These countermeasures are required. When a radio frequency cordless accessory such as a keyboard or a mouse is used, separate it 5 meters from RED equipment. Radio frequency cordless accessories cannot be used to process classified information unless encrypted.

**3.4.8 Wireless Local Area Networks (LAN).** These countermeasures are required. When a radio frequency wireless LAN is used, separate the transmitter and receiver units 5 meters from RED equipment.

**3.4.9 Infrared LANs.** These countermeasures are required. An infrared LAN processing classified information requires blocking the line of sight to a possible place where an adversary could detect the infrared emanations. Do not forget that smooth or shiny surfaces cause infrared signals to be reflected. The best solution is to use a closed room, keeping the doors closed and covering the windows with drapes.

**3.4.10 Infrared Devices.** These countermeasures are required. Infrared devices not covered by any subparagraph of paragraph 3.4 requires blocking the line of sight to a possible place where an adversary could detect the infrared emanations. Do not forget that smooth or shiny surfaces cause infrared signals to be reflected. The best solution is to use a closed room, keeping the doors closed and covering the windows with drapes.

**NOTE:** If guidance in paragraph 3.3 on Alarm signals is needed, please contact the Program Manager/Contract Monitor to obtain.

Effective 11 December 2002

**ADDENDUM TO DD FORM 254 (Blk 111)**  
**NOTIFICATION OF WPAFB SERVICING SECURITY ACTIVITY**

1. Thirty days **before** the date Contractor operations will begin on Wright-Patterson AFB OH (WPAFB), the Contractor shall provide to 88 SFS/SFAS Bldg 8, 1801 Tenth Street, WPAFB, OH 45433-7625 the following information:

a. The name, address, and telephone number of your company's Facility Security Officer and your designated on-site security representative;

b. The contract number and military contracting command;

c. The highest classification category of defense information to which Contractor employees will have access;

d. The date Contractor operations will begin on WPAFB OH;

e. The estimated completion date of operations on WPAFB OH;

2. This requirement is in **addition** to visit request notification procedures contained in DoD 5220.22M, National Industrial Security Program Operating Manual, Chapter 6.

Effective 12 February 2002

**ADDENDUM TO DD FORM 254 (Block 11i)**  
**EMISSION SECURITY (EMSEC) REQUIREMENTS**  
**(FORMERLY TEMPEST REQUIREMENTS)**

**EMISSIONS SECURITY ASSESSMENT REQUEST (ESAR)**

**FOR ALL CLASSIFIED SYSTEMS**

1. The contractor shall ensure that compromising emanations (EMSEC) conditions related to this contract are minimized.
2. The contractor shall provide countermeasure assessment data to the Contracting Officer (CO), **in accordance with Chapter 8 of the NISPOM Supplement**, in the form of an ESAR. The ESAR shall provide only specific responses to the data required in paragraph 3 below. The contractor's standard security plan shall **NOT** be used as a "stand-alone" ESAR response. The contractor shall **NOT** submit a detailed facility analysis/assessment. The ESAR information will be used to complete an EMSEC Countermeasures Assessment Review of the contractor's facility to be performed by the government EMSEC authority using current Air Force EMSEC directives. EMSEC is applied on a case-by-case basis and further information may be required to complete the review. The contractor shall provide this information to the CO when requested. After the evaluation of the ESAR by the government EMSEC authority, additional EMSEC requirements may be necessary. When changes to the information required in paragraph 3 below occurs (including, but not limited to, relocation, additions, or deletions of equipment from the original approved room), the contractors shall notify the CO of these changes. Upon request, the contractor shall submit to the CO a new ESAR, identifying the new configuration at least 30 days before the change occurs. The contractor shall **NOT** commence processing with the new configuration until receiving, as a minimum, interim approval from the CO.
3. \*ESAR contents shall include, as a minimum, the following information:
  - a. The specific classification and special categories of material to be processed/handled by electronic means. Include percentage of each classification level used including unclassified (i.e., 5% Top Secret, 10% Secret/SAR, 25% Secret, 60% Unclassified).
  - b. The specific location (complete address, building/room number, or office) where classified processing will be performed. Include identification of any other contractor/company located within 200 meters of the facility.
  - c. Attach a copy of the Defense Investigative Service (DIS) Form 147 to validate physical security and approved storage level of the facility.
  - d. Provide the name, title, and telephone number (commercial and/or DSN) of a point of contact at the facility where processing will occur.
4. The prime contractor shall ensure that all subcontractors and/or vendors comply with EMSEC requirements when performing classified processing related to this contract. The subcontractor will provide the above documentation through their prime to the CO to complete the ESAR.
5. **In addition** to the information required for all classified systems, the following will be required for **Top Secret** processing:
  - a. Identify the radius (in meters) of the physical control space available around the system, equipment, or facility. Describe the barriers, doors, fences, walls, etc that define the area. Describe the control exercised over the area during duty and nonduty hours. Describe other factors, which contribute to control (i.e., visitor procedures, escort requirements, searches of personnel and/or vehicles, etc).
  - b. Identify the type and location (relative to the classified system) of any unfiltered/telephone or communication lines, shielded or unshielded twisted pair cables or fiber, underground or unfiltered power lines, conduit, heating and air conditioning ducts, water pipes, etc, that transgress the established controlled area.
  - c. Describe the building in which the classified system(s) is housed, i.e., concrete block outer walls, 2" X 4" and single ply gypsum board inner walls, true floor to true ceiling walls, metallic (steel) or solid wood doors, windows (if there are windows, describe the type of coverings on them), etc.
  - d. Diagrams and/or drawings would be extremely helpful.
6. Additional information may be requested upon review of the documentation provided.

**\*NOTE: A copy of your Automated Information System Security Plan(s) (AISSP) will suffice.**

Effective 18 July 2002